UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,563	02/18/2004	Venkatesh Veeraraghavan	50037.238US01	3537

27488 7590 02/20/2009

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
GUPTA, MUKTESH G	

ART UNIT	PAPER NUMBER
2444	

MAIL DATE	DELIVERY MODE
02/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/782,563	VEERARAGHAVAN ET AL.	
	Examiner	Art Unit	
	Muktesh G. Gupta	2444	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-11,14-19,22 and 23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-11, 14-19 and 22-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Amendments received on 12/04/2008 have been entered.

Claims 1-5, 7-11, 14-19 and 22-23 are amended.

Claims 6, 12-13 and 20-21 are cancelled.

Claims 1-5, 7-11, 14-19 and 22-23 have been examined on merits and are pending in this application.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/04/2008 has been entered.

Response to Arguments

3. Applicant's arguments with respect to pending claims have been considered but are moot in view of the new ground(s) of rejection.

   a. Applicant's arguments with respect to **Claim 1** have been considered but are moot in view of the new ground(s) of rejection.

   b. Applicant's arguments and amendments filed on 12/04/2008 have been carefully considered but they are deemed moot in view of the following new

grounds of rejection as explained here below, necessitated by Applicant's substantial amendment to the claims "*receiving rules from an administration client computing device, the rules comprising query criteria for the audience, each rule defined as a unit of functionality; using the received rules to determine a membership list of the plurality of users to receive the content, the received rules comprising a property query rule, a member of rule, and a reports under rule, by: independently generating separate results of the property query rule by determining if a property value matches a property of one or more of the plurality of users in one or more preexisting lists; independently generating separate results of the a member of rule by determining if one or more of the plurality of users are a member of a particular preexisting list among the one or more preexisting lists; and independently generating separate results of the a reports under rule by determining if one or more of the plurality of users are located hierarchically under another user within a the one or more preexisting lists wherein the one or more preexisting lists include a group distribution list, a security group and an organizational structure; and after independently generating the separate results of each of the property query rule, the member of rule, and the reports under rule, compiling the membership list of users by applying one or more conditional logic operators to combine the separate results of the property query rule, the separate results of the member of rule, and the separate results of the reports under rule; associating the compiled membership list of*

users with content; obtaining the content from a data store; and providing the content to the users listed within the compiled membership list, which significantly affected the scope thereof.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. ***Claims 1-5, 7-11, 14-19 and 22-23*** *are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 6460141 to Olden; Eric M. (hereinafter "Olden").*

As to Claims 1, 10 and 16 *Olden disclose method, system and computer program for targeting content to an audience that comprises a plurality of users, the method comprising (as stated in col. 4, lines 55-57, lines 1-6, lines 13-18,* As shown in FIG. 1, the Web servers 20A, 20B, 20C provide Web-enabled applications and content to computer network users. Preferred configuration is as shown in FIG. 1, in which the security and access management system 10 comprises the plurality of authorization servers 24A, 24B, 24C and authorization dispatchers 26A, 26B, which operate in conjunction to provide efficient scalability of authorization requests. One of the

authorization servers 24A, 24B, 24C communicates with an enabled Web server 20A, 20B, 20C and the authorization dispatchers 26A and 26B over a socket connection. The authorization servers 24A, 24B, 24C communicate with the entitlements server component 14 over a CORBA ORB (Object Request Broker)):

receiving rules from an administration client computing device, the rules comprising query criteria for the audience, each rule defined as a unit of functionality (as stated in col. 2, lines 66-67, col. 19, lines 3-15, FIG. 4 illustrates the data model architecture of the security and access management system for one embodiment of business rules to process user requests for access to application functions. Smart rules can be used to automate the access privilege enforcement. A smart rule is defined that determines which properties (characteristics) of a user need be present in order to be given access. Smart rules essentially build access control lists dynamically based on the properties of the users. In order for a smart rule to operate against a particular property, the smart rule must first be defined in the entitlements database 32. The properties of a user are such things as "job title" or "account balance" or "premium account holder" or "trustee");

using the received rules to determine a membership list of the plurality of users to receive the content, the received rules comprising a property query rule, a member of rule, and a reports under rule, by (as stated in col. 13, lines 23-49, col. 17, lines 14-26, The security and access management system 10 allows a security administrator to create an unlimited number of users, each with individual defining properties. The administrator can further collect users into groups and groups into realms. Additionally,

users can be in multiple groups. This feature is useful for administrators trying to mimic organizational structure (for example, user John Doe may be in the promotions group, which is in the marketing realm) or geography (user Jane Doe is in the Paris group, which is in the Europe realm), or any other type of grouping. The user/group/realm concept is also important for setting permissions and entitlements, as described in connection with the description of the Basic Entitlements page. Entitlements are defined and administered using the Basic Entitlements page, as shown in FIG. 17. By adding entitlements using the security and access management system 10, entitlements to particular applications can be assigned to users, groups, or realms with ease. First, the administrator selects the user, group, or realm to be granted the entitlement. This is similar to the selection process on the Users page, described earlier. The appropriate entity is then selected from the entity menu. Clicking the left Choose button brings up a list of all available users, groups, or realms. The entity to be administered is selected from this list, and the Choose button is clicked. All of the entitlements for the selected user, group, or realm appear in the Basic Entitlements list box);

independently generating separate results of the property query rule by determining if a property value matches a property of one or more of the plurality of users in one or more preexisting lists (as stated in col. 13, lines 37-49, col. 14, lines 33-49, In order to find a particular user, group, or realm in the list box, an administrator can scroll through the list of entities or use the Search function. The Search function is indexed differently depending on the type of entity selected. For users, the Search function indexes on last name. For groups and realms, the Search function indexes on

the group or realm name. In order to add users to a group, Users is selected in the entity menu. The user list appears in the entity list box. In order to set a property for a new user, the user is selected from the User list, and the Modify button is clicked to bring up the Modify User dialog window which is similar to the Create User window shown in FIG. 9, but contains the information that was entered when the user was created. The Property list contains all of the properties available for the selected user. In order to change a property Value, the Property is selected, and the Change Property Value button is clicked. The Enter Property dialog window then appears. A value can be entered for the property. The security and access management system 10 only allows valid property values to be entered, based on the property type (True or False for Boolean properties, integers for integer properties, real numbers for floating-point properties, dates for date properties, character strings for string properties, and null for properties that can be set to null);

independently generating separate results of the a member of rule by determining if one or more of the plurality of users are a member of a particular preexisting list among the one or more preexisting lists (as stated in col. 15, lines 12-19, in order to add users to a group, Users is selected in the entity menu. The user list appears in the entity list box. Then, the Select Group button is clicked. The Group List dialog window will appear. The group to be populated is then selected, and the OK button is clicked. In order to include users in that group, the user to be added is highlighted to select the user, and the Add Arrow button is then clicked);

and independently generating separate results of the a reports under rule by determining if one or more of the plurality of users are located hierarchically under another user within a the one or more preexisting lists wherein the one or more preexisting lists include a group distribution list, a security group and an organizational structure (as stated in col. 7, lines 42-48, col. 15, lines 26-46, col. 21, lines 15-21, The resource consumer architecture 56 also provides a containment hierarchy or containers 74 of users 68. This allows an administrator to more easily assign access rights to a large group of users 68 without having to assign rights individually. A user 68 can be grouped together into a group object 76. Group objects 76 likewise can be grouped together into a realm object 78. Adding groups to realms and removing groups from realms is similar. When Groups is selected in the entity menu, the Select Group button automatically changes to read Select Realm. The Select Realm button is clicked, and the realm to be changed is selected from the realm list dialog window. In order to add a group to that realm, the group to be added is highlighted to select the group, and the Add Arrow button is clicked. In order to delete a group from the realm, the group to be removed is highlighted to select the group, and the Remove Arrow button is clicked. In order to edit a user, group, or realm, Users, Groups, or Realms is selected from the entity menu. All of the available entities of that type then appear in the list box below. The user, group, or realm to be modified is then highlighted to select the entity, and then the Modify button is clicked. The Modify dialog window appears. The Modify dialog window is identical to the Create dialog window, but contains all of the current user/group/realm information, which can be edited. Once the fields in the Modify dialog

window have been changed, OK is clicked to complete the Modify, or the Cancel button is clicked to abort. An enterprise can create a hierarchical administration structure which allows for a grandparent.fwdarw.parent.fwdarw.child.fwdarw.grandchild type structure. Additionally, the enterprise can avoid being in the business of administration and is able to push administration of additional groups down the administration chain);

and after independently generating the separate results of each of the property query rule, the member of rule, and the reports under rule, compiling the membership list of users by applying one or more conditional logic operators to combine the separate results of the property query rule, the separate results of the member of rule, and the separate results of the reports under rule; associating the compiled membership list of users with content (as stated in col. 18, lines 21-56, Various steps are required to create a smart rule. Referring to FIG. 18, the first step in creating a smart rule is selecting the Application for which the smart rule is to be created. The application list will disappear, and all of the application functions for the selected application will appear in the Application Functions list box. The function to which the smart rule is to apply is then selected. From the User Properties list box, the user property to be examined is selected. In order to create the entitlement, the Left Arrow button is clicked. This brings up the smart rules filter box, as shown in FIG. 19. The smart rules filter box shown in FIG. 19 is employed to create a filter. A filter comprises four components, namely, a rule type, a property, an operator, and a Value. The rule is selected from the rule list, which is a pull-down list beside the word Define. As described above, the rule is either Require, Deny, or Allow. The property is the property selected on the smart rules main

page shown in FIG. 18. The operator is selected from the operator pull-down menu. The available operators depend on the type of property. Integer properties (INT) have mathematical operators, such as >(greater than); <(less than); =(equal to); !=(not equal to); >=(greater than or equal to); and <=(less than or equal to). Floating-point properties (FLOAT) have the following mathematical operators: >(greater than); <(less than); =(equal to); !=(not equal to); >=(greater than or equal to); and <=(less than or equal to). Boolean properties (BOOL) are either True or False. Their operators are IS or IS NOT. String properties (STRING) have the following operators: Contains, Does Not Contain, Ends With, Starts With, and Equals. Finally, date properties (DATE) have two operators, namely, BEFORE and AFTER. The BEFORE and AFTER properties are not inclusive);

obtaining the content from a data store (as stated in col. 19, lines 12-28, Smart rules essentially build access control lists dynamically based on the properties of the users. These properties most often reside in existing enterprise databases, such as customer list databases or employee databases. In order for a smart rule to operate against a particular property, the smart rule must first be defined in the entitlements database 32. Then, the properties from the customer or employee database can be loaded into the entitlements database 32, and synchronized periodically to keep them up to date. This can be easily done through the bulk loading function of the API server 16. Once the user properties have been extended and populated, the process of building smart rules begins. These smart rules are dynamic, since they are applied to properties which are continually updated through the bulk loading function);

and providing the content to the users listed within the compiled membership list. (as stated in col. 17, lines 66-67, col. 18, lines 1-4, Smart rules are filters that govern user access to applications. When a smart rule is defined for an application, in order to determine authorization, the security and access management system 10 examines a property for a specific user, and grants or denies access to an application resource based on the value that is found).

As to Claims 2, 11 and 17-18 *Olden disclose method, system and computer program of Claims 1, 10 and 16, wherein the rules to define the audience further comprises an attribute (as stated in col. 7, lines 26-41,* Specifically, as shown in FIG. 2, the resource consumer architecture 56 comprises a consumer architecture which is divided into a consumer object model 64 and an extensible consumer attribute model 66. A consumer object is referred to as a user 68. A user 68 has several defined attributes (for example, user ID, first name, last name, password, etc.), as well as extendible attributes. These extendible attributes are referred to as user properties 70. The name and type of a user property 70 (for example, a string property, a date property, and integer property, etc.) is defined by a user property definition 72. When a user property definition 72 is created, all users 68 automatically inherit a user property 70 of the defined name and type. However, a value is not automatically assigned to a user property 70. A user property definition 72 preferably includes at least one of the following types: Boolean; string; integer; floating point; and date);

a member; and an organization (as stated in col. 7, lines 42-48, The resource consumer architecture 56 also provides a containment hierarchy or containers 74 of users 68. This allows an administrator to more easily assign access rights to a large group of users 68 without having to assign rights individually. A user 68 can be grouped together into a group object 76. Group objects 76 likewise can be grouped together into a realm object 78).

As to Claims 3, 15 and 23 *Olden disclose method, system and computer program of Claims 1, 10 and 16, wherein the content is provided within a web part (as stated in col. 7, lines 11-48, col. 8, lines 34-43,* a resource consumer is someone who accesses or manipulates a defined resource. Generally, a resource consumer is someone who requests access to a Web-enabled or non-Web-enabled application or content. For example, a resource consumer could be an employee who needs to retrieve sensitive documents, a customer who wishes to modify his or her account information, or a supplier with rights to view. Referring again to FIG. 2, the resource definition architecture 60 comprises an application architecture 86 which groups protected resources into applications 88. A Web-based application 88 is comprised of Uniform Resource Identifiers (URIs) 90. Other types of applications do not have resources directly contained in the application; rather, the application represents implicitly a group of resources. Applications 88 also have associated application functions 84, which represent the various services associated with an application).

As to Claims 4-5 and 19 *Olden disclose method and computer program of Claims 1 and 16, wherein the organization structure is stored in a directory service (as stated in col. 12, lines 18-36, col. 13, lines 23-29,* The operation of the administrative client 18 shown in FIG. 1 the entitlements manager software for the security and access management system 10 is launched, which causes a login window to be displayed, as shown in FIG. 6. In the case that the security and access management system 10 is running on a Windows 95/NT platform, there are two options to launch the entitlements manager. The first option is to select an entitlements manager icon from the start menu.fwdarw.programs. The second option is to double click a clrtrustmgr.bat file under the directory for the entitlements manager for the security and access management system 10. The security and access management system 10 allows a security administrator to create an unlimited number of users, each with individual defining properties. The administrator can further collect users into groups and groups into realms. Additionally, users can be in multiple groups. This feature is useful for administrators trying to mimic organizational structure).

As to Claims 7, 14 and 22 *Olden disclose method, system and computer program of Claims 1, 10 and 16, further comprising scheduling the compilation of the rules on a predetermined time schedule (as stated in col. 19, lines 12-28,* Smart rules essentially build access control lists dynamically based on the properties of the users. The properties of a user are such things as "job title" or "account balance" or "premium account holder" or "trustee." Properties are nouns which are used in day-to-day

business operations. These properties most often reside in existing enterprise databases, such as customer list databases or employee databases. In order for a smart rule to operate against a particular property, the smart rule must first be defined in the entitlements database 32. Then, the properties from the customer or employee database can be loaded into the entitlements database 32, and synchronized periodically to keep them up to date. This can be easily done through the bulk loading function of the API server 16. Once the user properties have been extended and populated, the process of building smart rules begins. These smart rules are dynamic, since they are applied to properties which are continually updated through the bulk loading function).

As to Claim 8 *Olden disclose method of Claim 1, further comprising providing access to the content through a web interface that is created individually for that audience member (as stated in col. 24, lines 1-13,* Referring to FIG. 30, the single sign on process is as follows. 1) The browser requests secured content from protected Web server 20A. 2) The plug-in for Web server 20A checks for a cookie. 3) Because this is the first authentication, the user provides his or her username and password. 4) User permissions are checked. 5) A cookie is built and set for the browser. 6) The Web user accesses protected Web server 20B. 7) The plug-in for Web server 20B uses the cookie for authentication. 8) Permissions are checked for the user based on the user's credentials contained in the cookie).

As to Claim 9 *Olden disclose method of Claim 1, further comprising storing the rules to define the audience as an XML representation (as stated in col. 22, lines 48-61,* A user property can also be modified. After selecting the property to be modified, clicking the Modify button on the User Properties page shown in FIG. 26 brings up a Modify User Property dialog window. This window is identical to the Create User Property dialog window shown in FIG. 27, but the details of the selected user property are included and can be edited. Once the user property has been changed as needed, clicking the Save button saves the changes, and clicking the Cancel button aborts. Some characteristics of the property, specifically Owner, can only be changed by administrators with special permissions (specifically, the ability to Modify Ownership, set on the Administrators page). User Properties can only be set for existing users, by modifying that user on the Users Page).

Remarks

5. The following pertaining arts are discovered and not used in this office action. Office reserves the right to use these arts in later actions.

a. Ben-Shaul, Israel et al. (US 20020010798 A1) Differentiated content and application delivery via internet

b. Bentolila, Isaac et al. (US 20030101451 A1) System, method, and software application for targeted advertising via behavioral model clustering, and preference programming based on behavioral model clusters

c. Mullins, Ward et al. (US 20030208505 A1) Dynamic class inheritance and distributed caching with object relational mapping and cartesian model support in a database manipulation and mapping system

d. O'Brien; Sean M. et al. (US 20060140134 A1) Advertising business method and system for secure and high speed transmission of media files across an internet, intranet or cable network, and method to avoid digital file sharing or copying

e. Yeager, William J. et al. (US 20040088348 A1) Managing distribution of content using mobile agents in peer-to peer networks

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Muktesh G. Gupta whose telephone number is 571-270-5011. The examiner can normally be reached on Monday-Friday, 8:00 a.m. -5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William C. Vaughn can be reached on 571-272-3922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MG

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2444